FIG.1

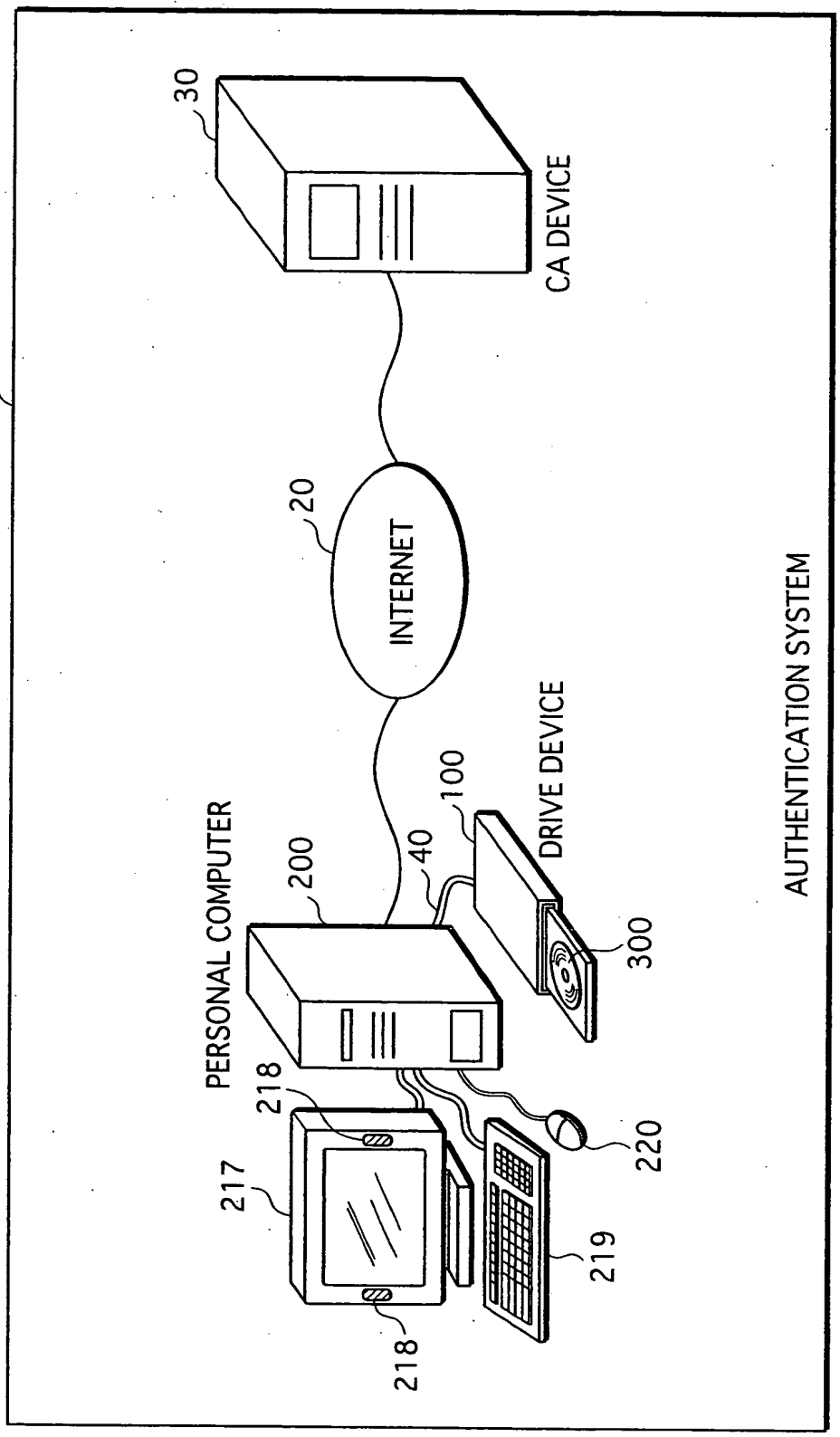

10
AUTHENTICATION SYSTEM
30
CA DEVICE
20
INTERNET
100
DRIVE DEVICE
300
40
200
PERSONAL COMPUTER
218
217
218
219
220

FIG.2

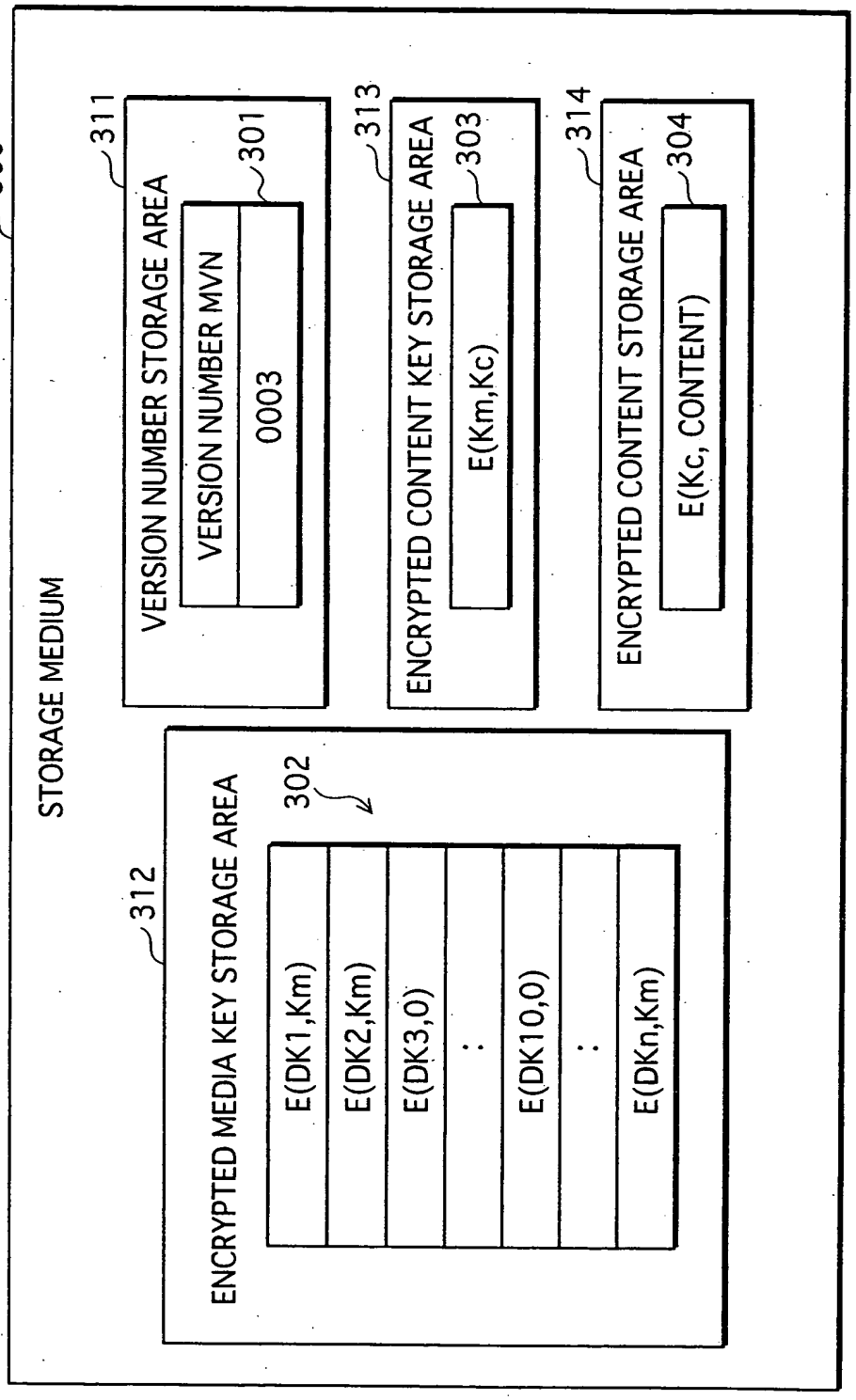

300
STORAGE MEDIUM
311
VERSION NUMBER STORAGE AREA
VERSION NUMBER MVN
0003
301
313
ENCRYPTED CONTENT KEY STORAGE AREA
E(Km,Kc)
303
314
ENCRYPTED CONTENT STORAGE AREA
E(Kc, CONTENT)
304
312
ENCRYPTED MEDIA KEY STORAGE AREA
302
E(DK1,Km)
E(DK2,Km)
E(DK3,0)
E(DK10,0)
E(DKn,Km)

FIG.3

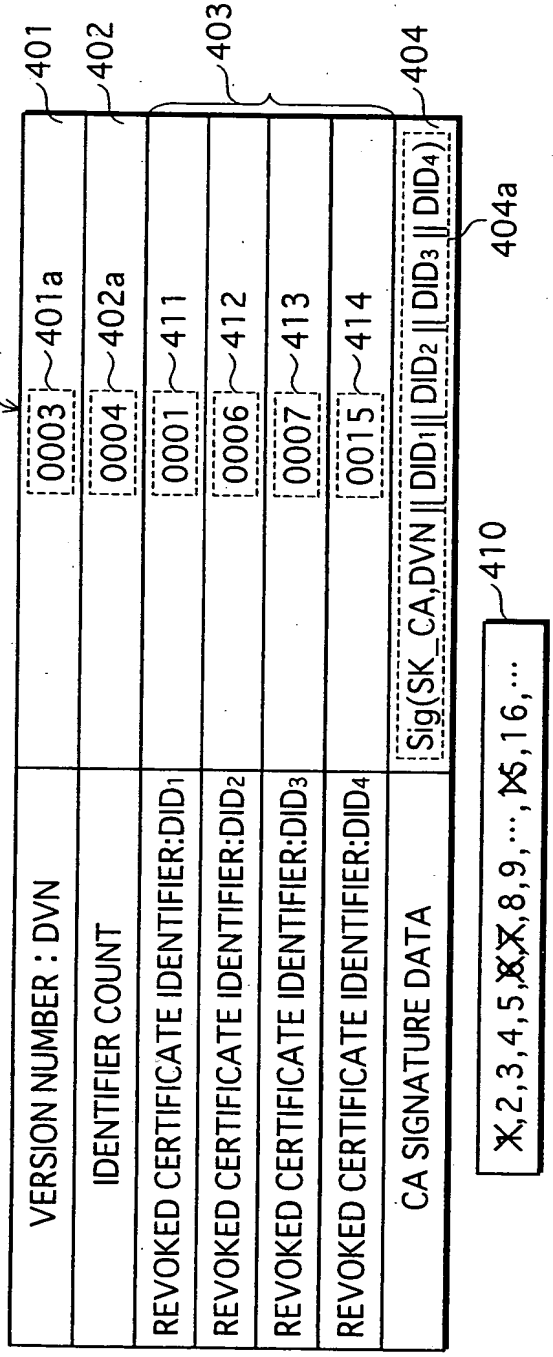

400
LIST D
VERSION NUMBER : DVN
IDENTIFIER COUNT
REVOKED CERTIFICATE IDENTIFIER:DID1
REVOKED CERTIFICATE IDENTIFIER:DID2
REVOKED CERTIFICATE IDENTIFIER:DID3
REVOKED CERTIFICATE IDENTIFIER:DID4
CA SIGNATURE DATA
0003
0004
0001
0006
0007
0015
Sig(SK_CA,DVN || DID1|| DID2 || DID3 || DID4)
401
401a
402
402a
403
411
412
413
414
404
404a
410
X,2,3,4,5,X,X,8,9,…,X,16,…

FIG.4

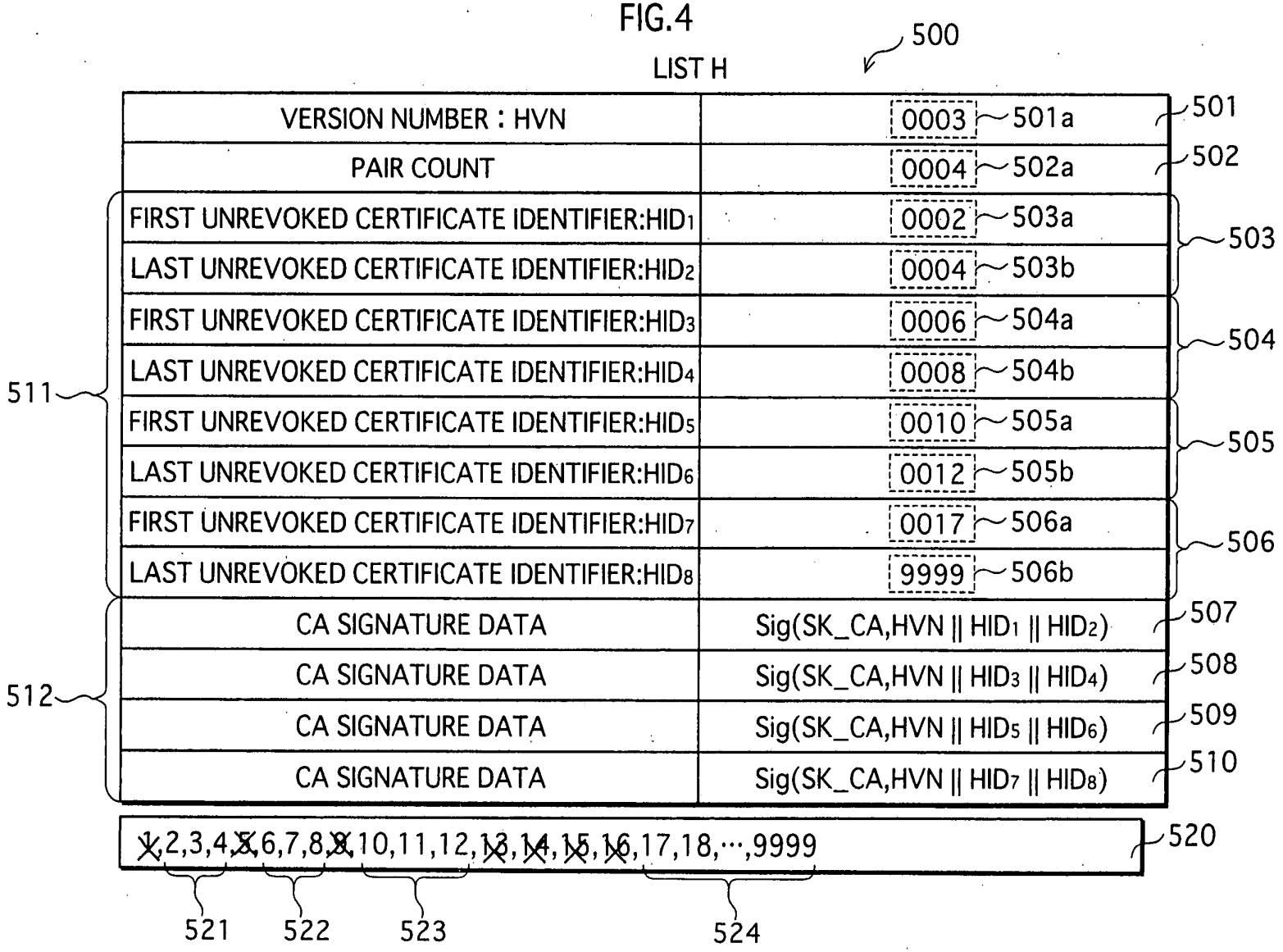

500
LIST H
VERSION NUMBER : HVN
0003
501a
501
PAIR COUNT
0004
502a
502
FIRST UNREVOKED CERTIFICATE IDENTIFIER:HID1
0002
503a
LAST UNREVOKED CERTIFICATE IDENTIFIER:HID2
0004
503b
503
FIRST UNREVOKED CERTIFICATE IDENTIFIER:HID3
0006
504a
LAST UNREVOKED CERTIFICATE IDENTIFIER:HID4
0008
504b
504
511
FIRST UNREVOKED CERTIFICATE IDENTIFIER:HID5
0010
505a
LAST UNREVOKED CERTIFICATE IDENTIFIER:HID6
0012
505b
505
FIRST UNREVOKED CERTIFICATE IDENTIFIER:HID7
0017
506a
LAST UNREVOKED CERTIFICATE IDENTIFIER:HID8
9999
506b
506
CA SIGNATURE DATA
Sig(SK_CA,HVN || HID1 || HID2)
507
CA SIGNATURE DATA
Sig(SK_CA,HVN || HID3 || HID4)
508
512
CA SIGNATURE DATA
Sig(SK_CA,HVN || HID5 || HID6)
509
CA SIGNATURE DATA
Sig(SK_CA,HVN || HID7 || HID8)
510
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,…,9999
520
521
522
523
524

FIG.5

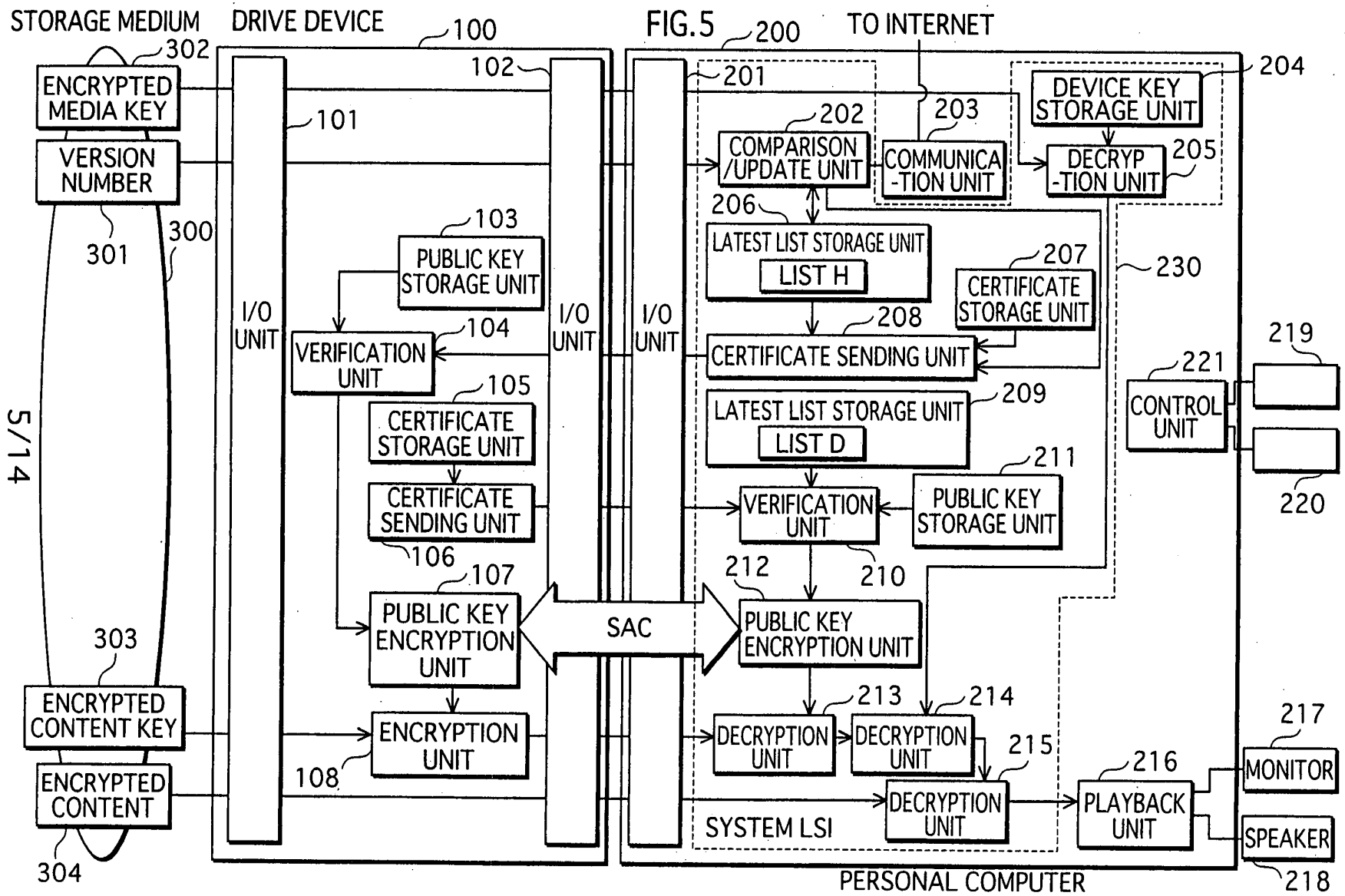

STORAGE MEDIUM
DRIVE DEVICE
100
200
TO INTERNET
302
ENCRYPTED MEDIA KEY
VERSION NUMBER
301
300
303
ENCRYPTED CONTENT KEY
ENCRYPTED CONTENT
304
I/O UNIT
101
102
I/O UNIT
I/O UNIT
201
202
COMPARISON /UPDATE UNIT
203
COMMUNICA -TION UNIT
204
DEVICE KEY STORAGE UNIT
DECRYP -TION UNIT
205
206
LATEST LIST STORAGE UNIT
LIST H
207
CERTIFICATE STORAGE UNIT
230
103
PUBLIC KEY STORAGE UNIT
104
VERIFICATION UNIT
208
CERTIFICATE SENDING UNIT
105
CERTIFICATE STORAGE UNIT
209
LATEST LIST STORAGE UNIT
LIST D
CERTIFICATE SENDING UNIT
106
211
VERIFICATION UNIT
PUBLIC KEY STORAGE UNIT
210
107
212
PUBLIC KEY ENCRYPTION UNIT
SAC
PUBLIC KEY ENCRYPTION UNIT
213
214
ENCRYPTION UNIT
108
DECRYPTION UNIT
DECRYPTION UNIT
215
DECRYPTION UNIT
SYSTEM LSI
216
PLAYBACK UNIT
217
MONITOR
SPEAKER
218
219
CONTROL UNIT
221
220
PERSONAL COMPUTER

FIG.6

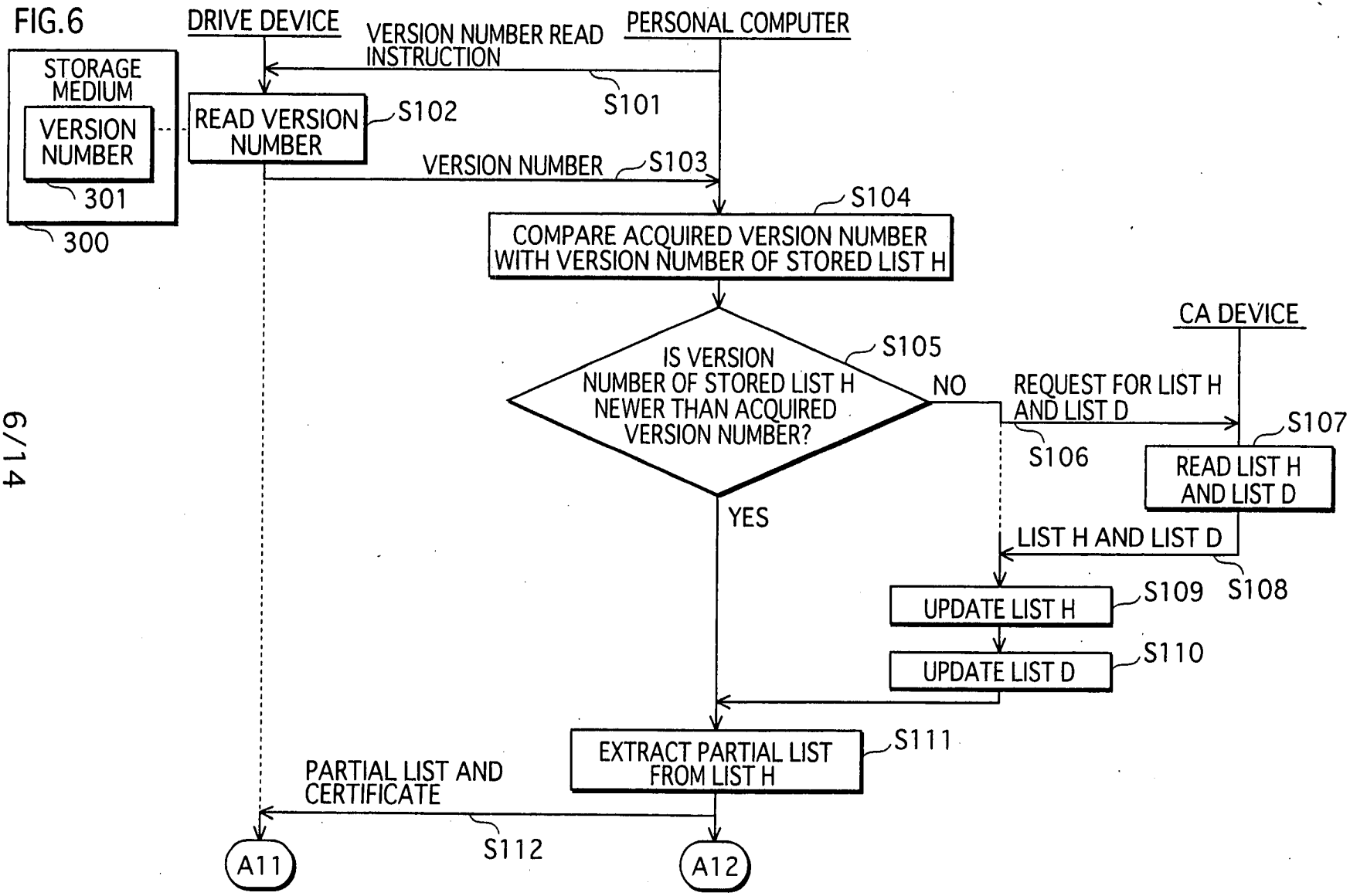

DRIVE DEVICE
PERSONAL COMPUTER
VERSION NUMBER READ INSTRUCTION
S101
STORAGE MEDIUM
VERSION NUMBER
301
300
READ VERSION NUMBER
S102
VERSION NUMBER
S103
S104
COMPARE ACQUIRED VERSION NUMBER WITH VERSION NUMBER OF STORED LIST H
CA DEVICE
S105
IS VERSION NUMBER OF STORED LIST H NEWER THAN ACQUIRED VERSION NUMBER?
NO
REQUEST FOR LIST H AND LIST D
S106
S107
READ LIST H AND LIST D
YES
LIST H AND LIST D
S108
UPDATE LIST H
S109
UPDATE LIST D
S110
EXTRACT PARTIAL LIST FROM LIST H
S111
PARTIAL LIST AND CERTIFICATE
S112
A11
A12

FIG.7

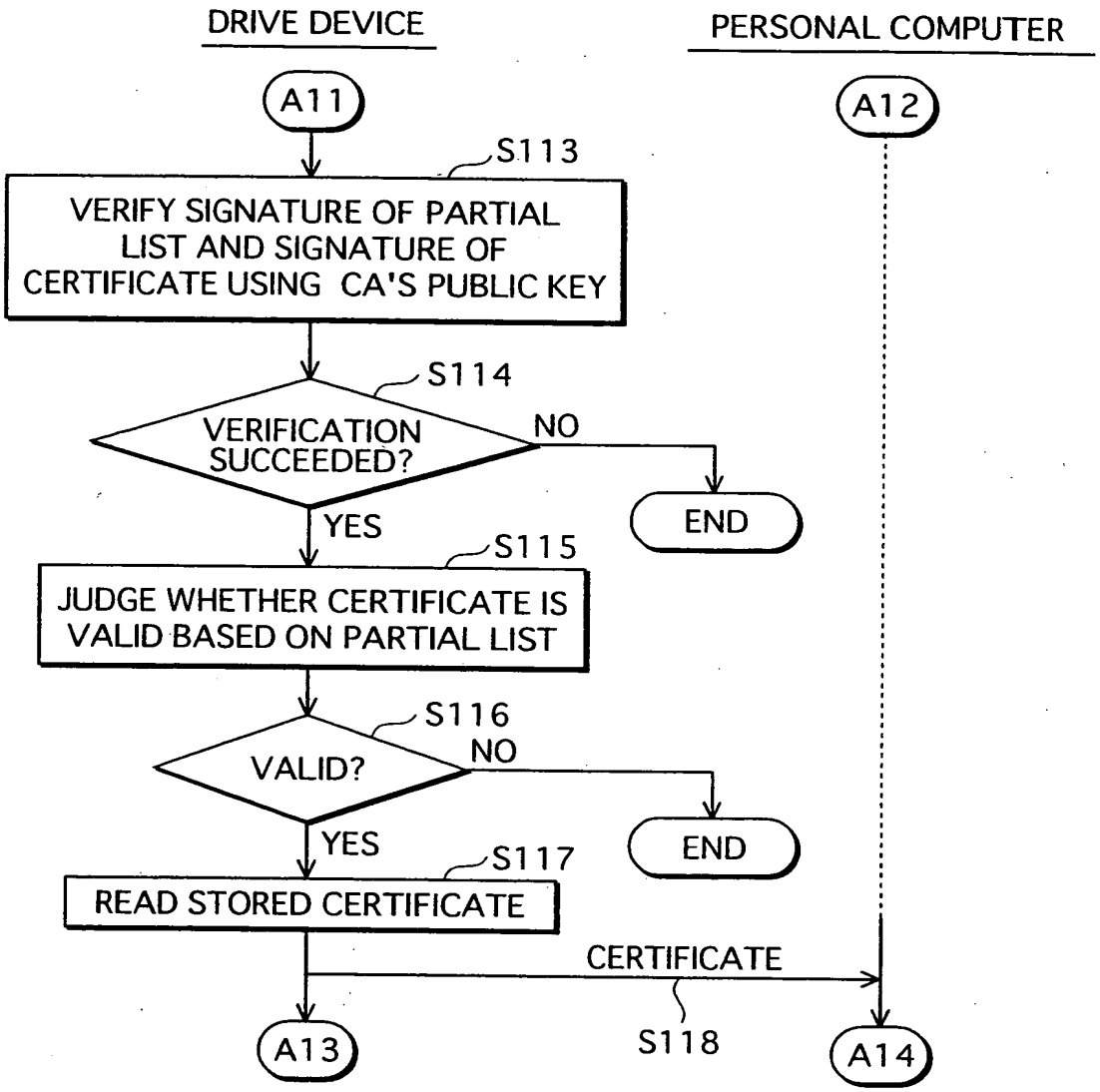

DRIVE DEVICE
PERSONAL COMPUTER
A11
A12
S113
VERIFY SIGNATURE OF PARTIAL LIST AND SIGNATURE OF CERTIFICATE USING CA'S PUBLIC KEY
S114
VERIFICATION SUCCEEDED?
NO
END
YES
S115
JUDGE WHETHER CERTIFICATE IS VALID BASED ON PARTIAL LIST
S116
VALID?
NO
END
YES
S117
READ STORED CERTIFICATE
CERTIFICATE
S118
A13
A14

FIG.8

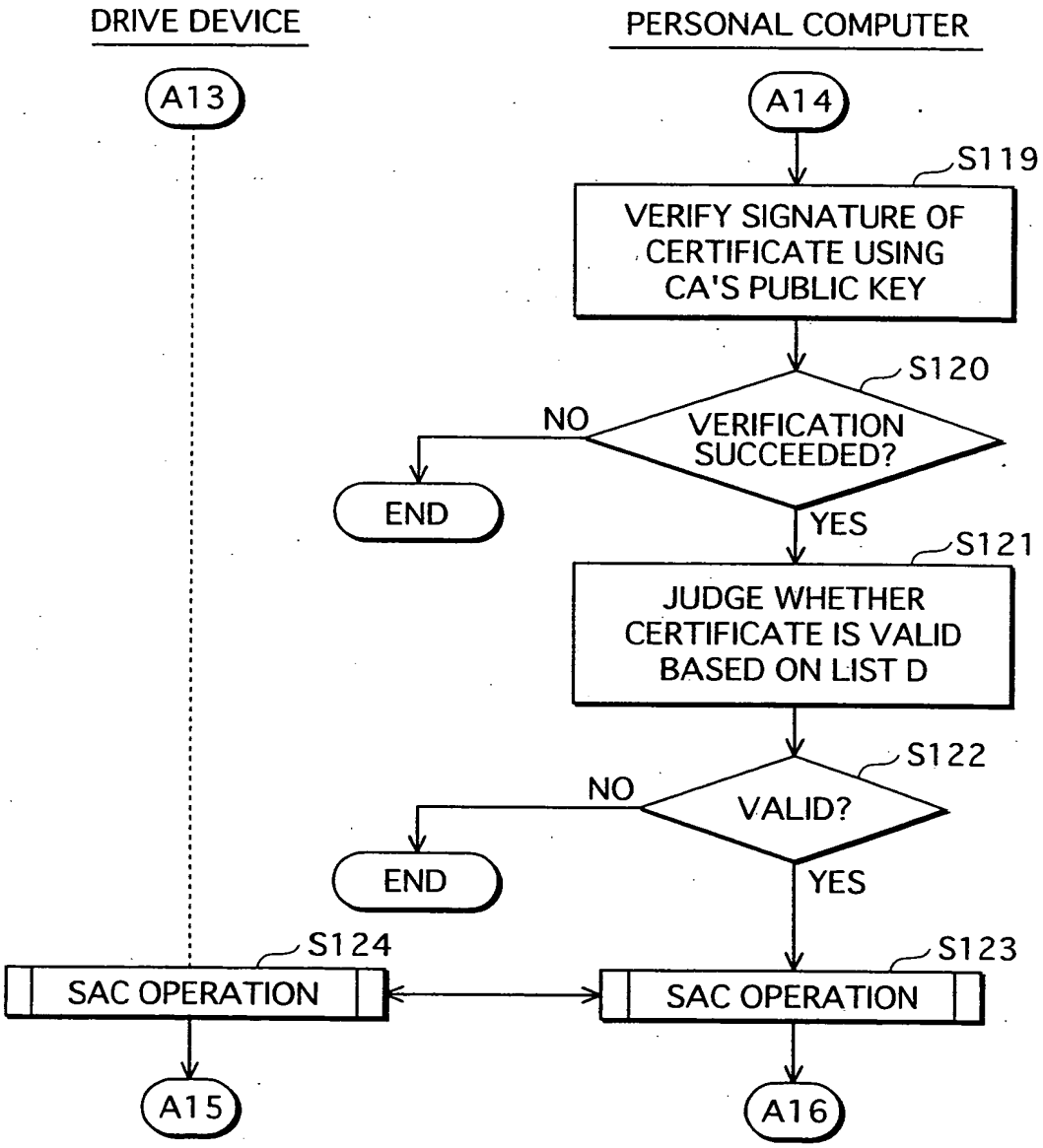

DRIVE DEVICE
PERSONAL COMPUTER
A13
A14
S119
VERIFY SIGNATURE OF CERTIFICATE USING CA'S PUBLIC KEY
S120
NO
VERIFICATION SUCCEEDED?
END
YES
S121
JUDGE WHETHER CERTIFICATE IS VALID BASED ON LIST D
S122
NO
VALID?
END
YES
S124
S123
SAC OPERATION
SAC OPERATION
A15
A16

FIG.9

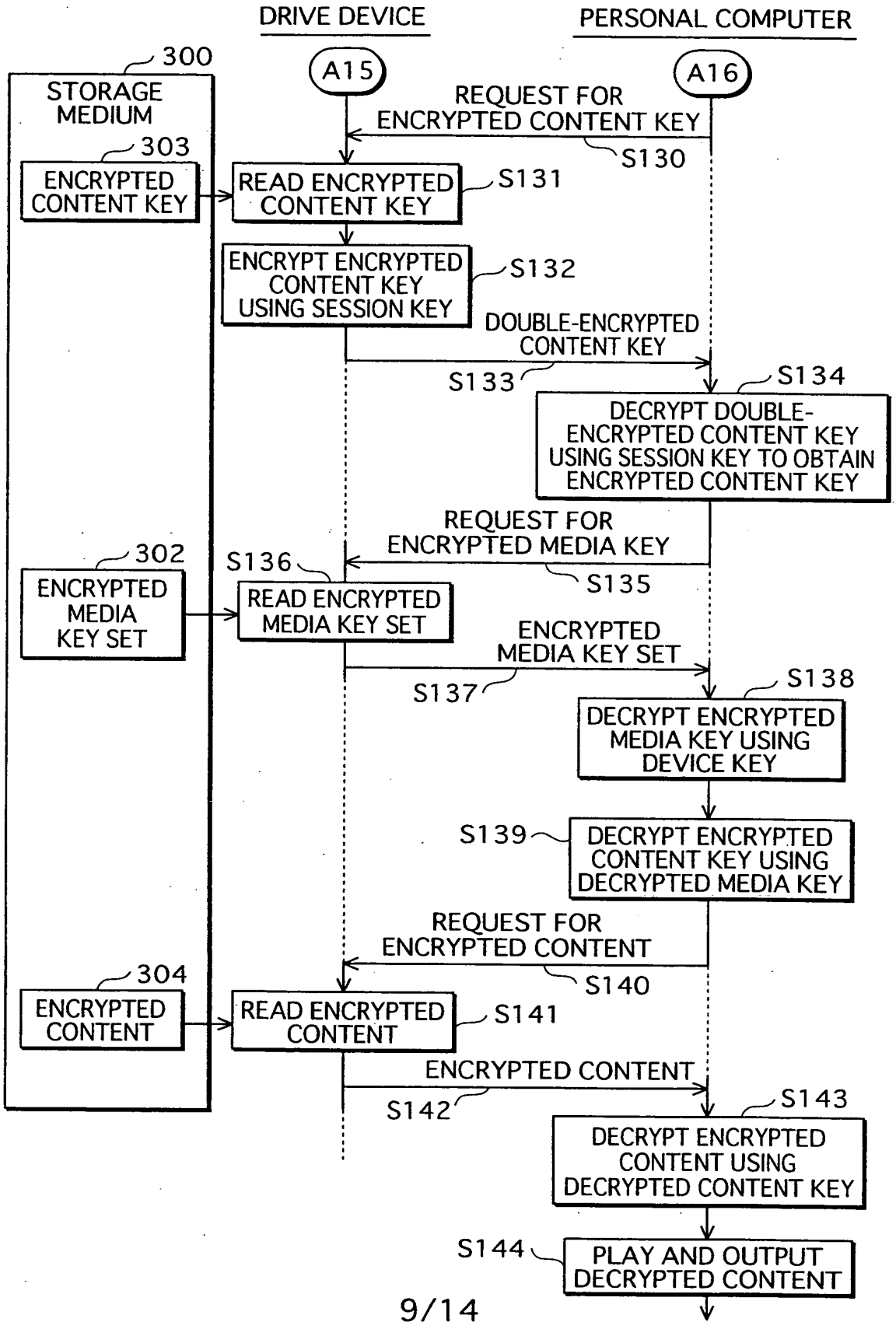

DRIVE DEVICE
PERSONAL COMPUTER
300
STORAGE MEDIUM
A15
A16
REQUEST FOR ENCRYPTED CONTENT KEY
S130
303
ENCRYPTED CONTENT KEY
READ ENCRYPTED CONTENT KEY
S131
ENCRYPT ENCRYPTED CONTENT KEY USING SESSION KEY
S132
DOUBLE-ENCRYPTED CONTENT KEY
S133
S134
DECRYPT DOUBLE-ENCRYPTED CONTENT KEY USING SESSION KEY TO OBTAIN ENCRYPTED CONTENT KEY
REQUEST FOR ENCRYPTED MEDIA KEY
S135
302
S136
ENCRYPTED MEDIA KEY SET
READ ENCRYPTED MEDIA KEY SET
ENCRYPTED MEDIA KEY SET
S137
S138
DECRYPT ENCRYPTED MEDIA KEY USING DEVICE KEY
S139
DECRYPT ENCRYPTED CONTENT KEY USING DECRYPTED MEDIA KEY
REQUEST FOR ENCRYPTED CONTENT
S140
304
ENCRYPTED CONTENT
READ ENCRYPTED CONTENT
S141
ENCRYPTED CONTENT
S142
S143
DECRYPT ENCRYPTED CONTENT USING DECRYPTED CONTENT KEY
S144
PLAY AND OUTPUT DECRYPTED CONTENT

FIG.10

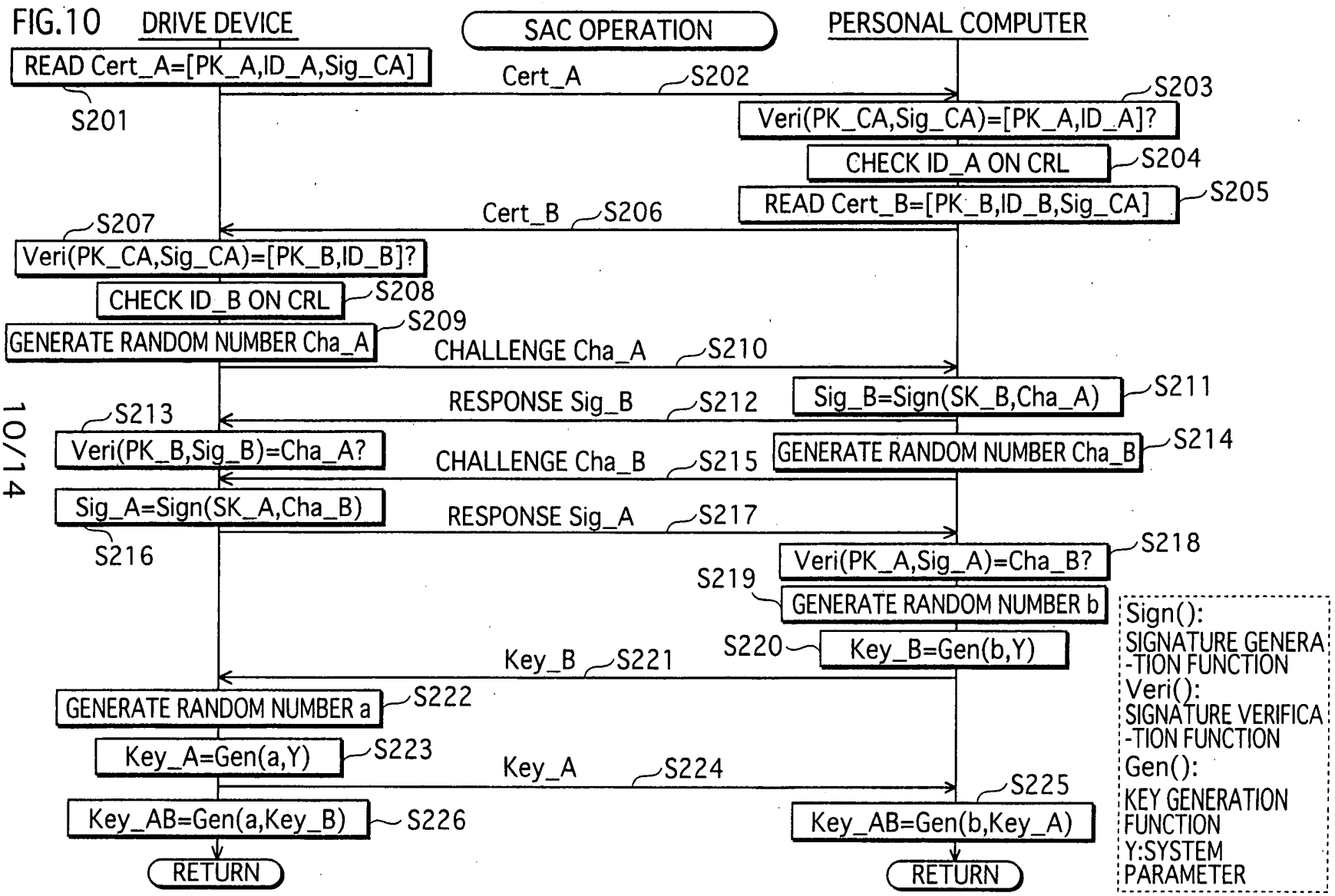

DRIVE DEVICE
SAC OPERATION
PERSONAL COMPUTER
READ Cert_A=[PK_A,ID_A,Sig_CA]
S201
Cert_A
S202
S203
Veri(PK_CA,Sig_CA)=[PK_A,ID_A]?
CHECK ID_A ON CRL
S204
READ Cert_B=[PK_B,ID_B,Sig_CA]
S205
Cert_B
S206
S207
Veri(PK_CA,Sig_CA)=[PK_B,ID_B]?
CHECK ID_B ON CRL
S208
GENERATE RANDOM NUMBER Cha_A
S209
CHALLENGE Cha_A
S210
Sig_B=Sign(SK_B,Cha_A)
S211
RESPONSE Sig_B
S212
S213
Veri(PK_B,Sig_B)=Cha_A?
GENERATE RANDOM NUMBER Cha_B
S214
CHALLENGE Cha_B
S215
Sig_A=Sign(SK_A,Cha_B)
S216
RESPONSE Sig_A
S217
Veri(PK_A,Sig_A)=Cha_B?
S218
S219
GENERATE RANDOM NUMBER b
S220
Key_B=Gen(b,Y)
Key_B
S221
GENERATE RANDOM NUMBER a
S222
Key_A=Gen(a,Y)
S223
Key_A
S224
S225
Key_AB=Gen(a,Key_B)
S226
Key_AB=Gen(b,Key_A)
RETURN
RETURN
Sign():
SIGNATURE GENERA-TION FUNCTION
Veri():
SIGNATURE VERIFICA-TION FUNCTION
Gen():
KEY GENERATION FUNCTION
Y:SYSTEM PARAMETER

FIG. 11

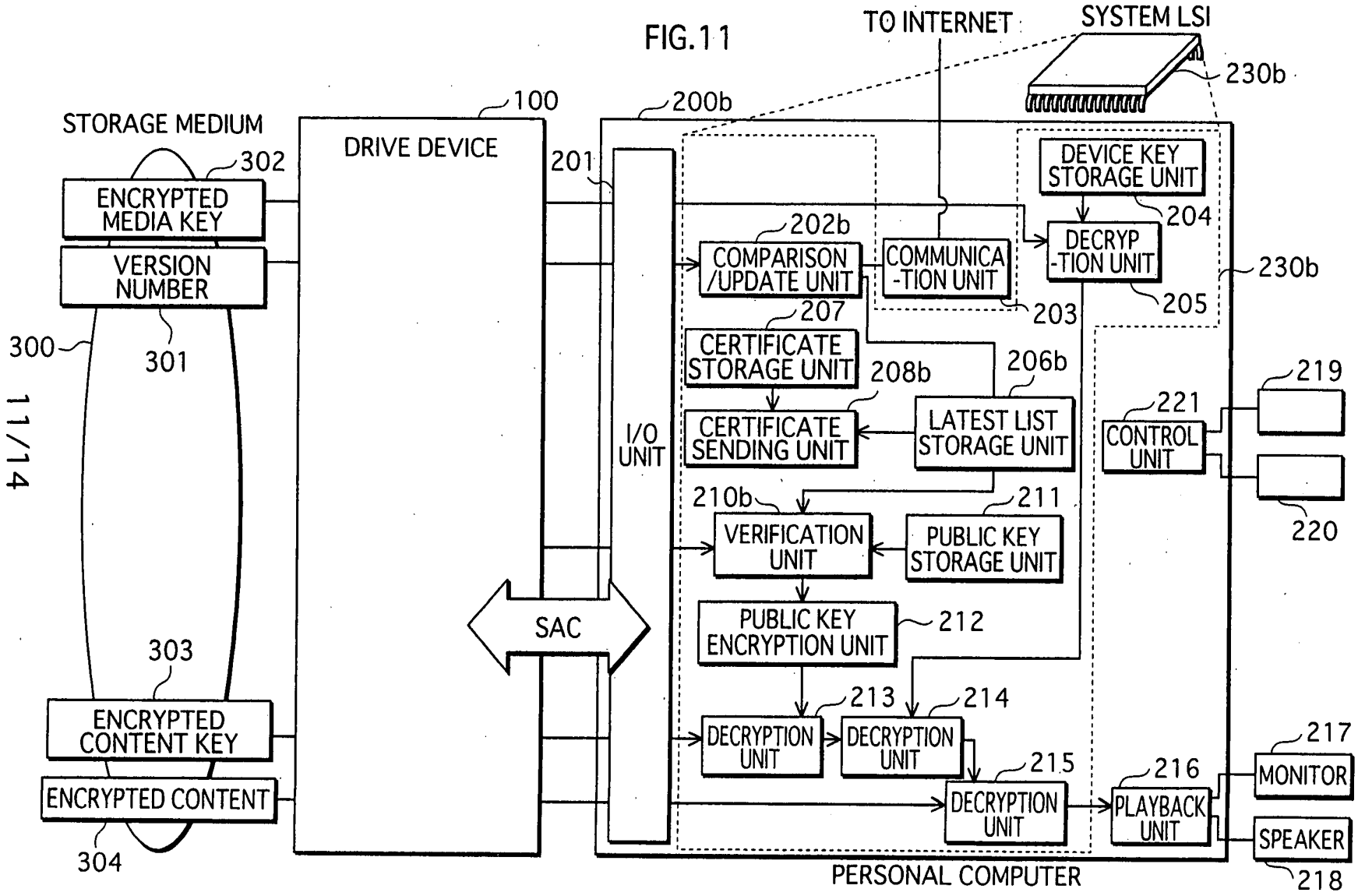

TO INTERNET
SYSTEM LSI
230b
STORAGE MEDIUM
100
DRIVE DEVICE
200b
201
302
ENCRYPTED MEDIA KEY
VERSION NUMBER
300
301
303
ENCRYPTED CONTENT KEY
ENCRYPTED CONTENT
304
I/O UNIT
SAC
DEVICE KEY STORAGE UNIT
204
DECRYP -TION UNIT
205
230b
202b
COMPARISON /UPDATE UNIT
COMMUNICA -TION UNIT
203
207
CERTIFICATE STORAGE UNIT
208b
206b
CERTIFICATE SENDING UNIT
LATEST LIST STORAGE UNIT
219
221
CONTROL UNIT
210b
211
VERIFICATION UNIT
PUBLIC KEY STORAGE UNIT
220
PUBLIC KEY ENCRYPTION UNIT
212
213
214
DECRYPTION UNIT
DECRYPTION UNIT
215
DECRYPTION UNIT
216
PLAYBACK UNIT
217
MONITOR
SPEAKER
218
PERSONAL COMPUTER

FIG.12

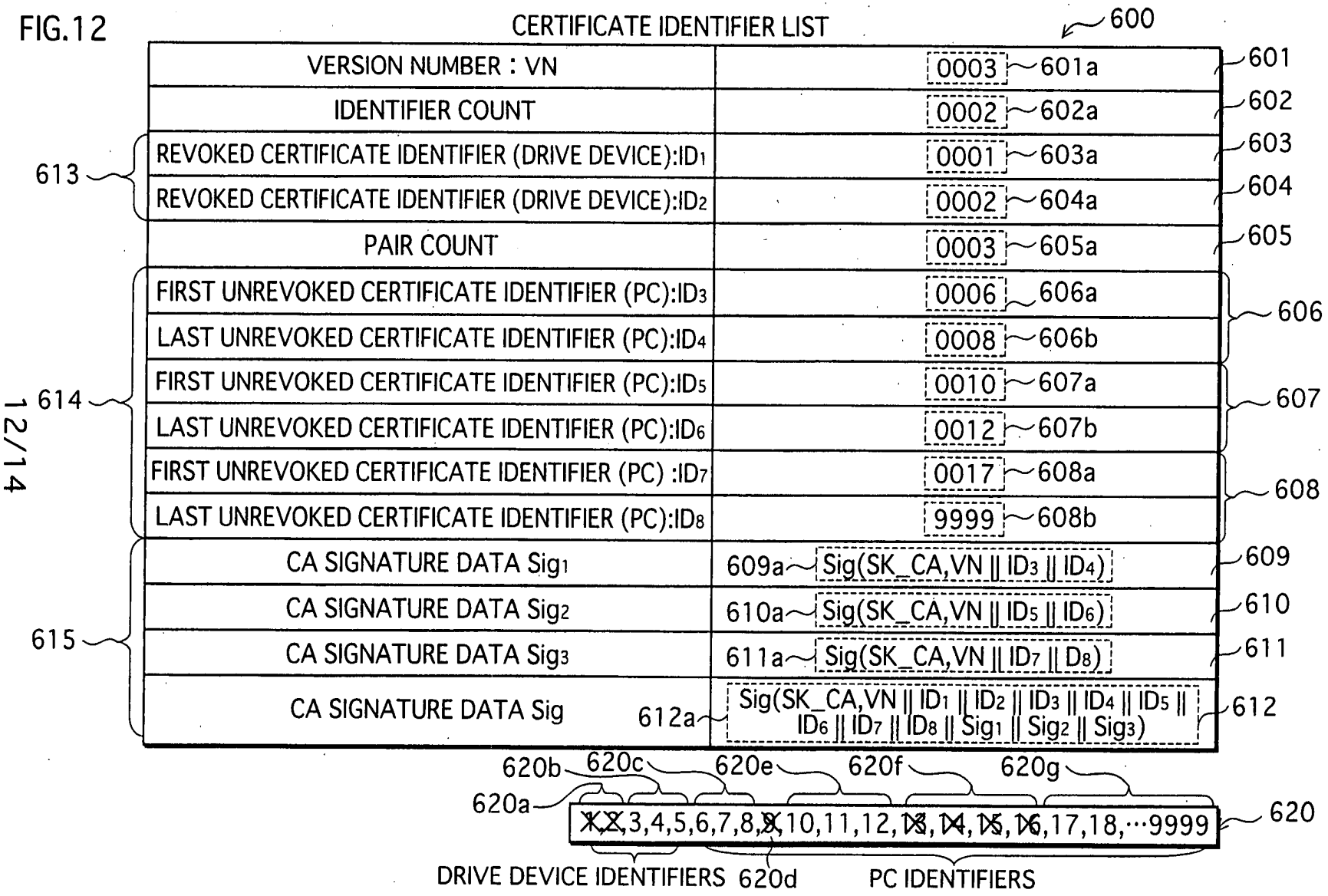

CERTIFICATE IDENTIFIER LIST
600
VERSION NUMBER : VN
0003
601a
601
IDENTIFIER COUNT
0002
602a
602
613
REVOKED CERTIFICATE IDENTIFIER (DRIVE DEVICE):ID1
0001
603a
603
REVOKED CERTIFICATE IDENTIFIER (DRIVE DEVICE):ID2
0002
604a
604
PAIR COUNT
0003
605a
605
FIRST UNREVOKED CERTIFICATE IDENTIFIER (PC):ID3
0006
606a
606
LAST UNREVOKED CERTIFICATE IDENTIFIER (PC):ID4
0008
606b
614
FIRST UNREVOKED CERTIFICATE IDENTIFIER (PC):ID5
0010
607a
607
LAST UNREVOKED CERTIFICATE IDENTIFIER (PC):ID6
0012
607b
FIRST UNREVOKED CERTIFICATE IDENTIFIER (PC) :ID7
0017
608a
608
LAST UNREVOKED CERTIFICATE IDENTIFIER (PC):ID8
9999
608b
CA SIGNATURE DATA Sig1
609a
Sig(SK_CA,VN || ID3 || ID4)
609
CA SIGNATURE DATA Sig2
610a
Sig(SK_CA,VN || ID5 || ID6)
610
615
CA SIGNATURE DATA Sig3
611a
Sig(SK_CA,VN || ID7 || D8)
611
CA SIGNATURE DATA Sig
612a
Sig(SK_CA,VN || ID1 || ID2 || ID3 || ID4 || ID5 || ID6 || ID7 || ID8 || Sig1 || Sig2 || Sig3)
612
620b
620c
620e
620f
620g
620a
XX,3,4,5,6,7,8,X,10,11,12,X,X,X,X,17,18,…9999
620
DRIVE DEVICE IDENTIFIERS
620d
PC IDENTIFIERS

FIG.13

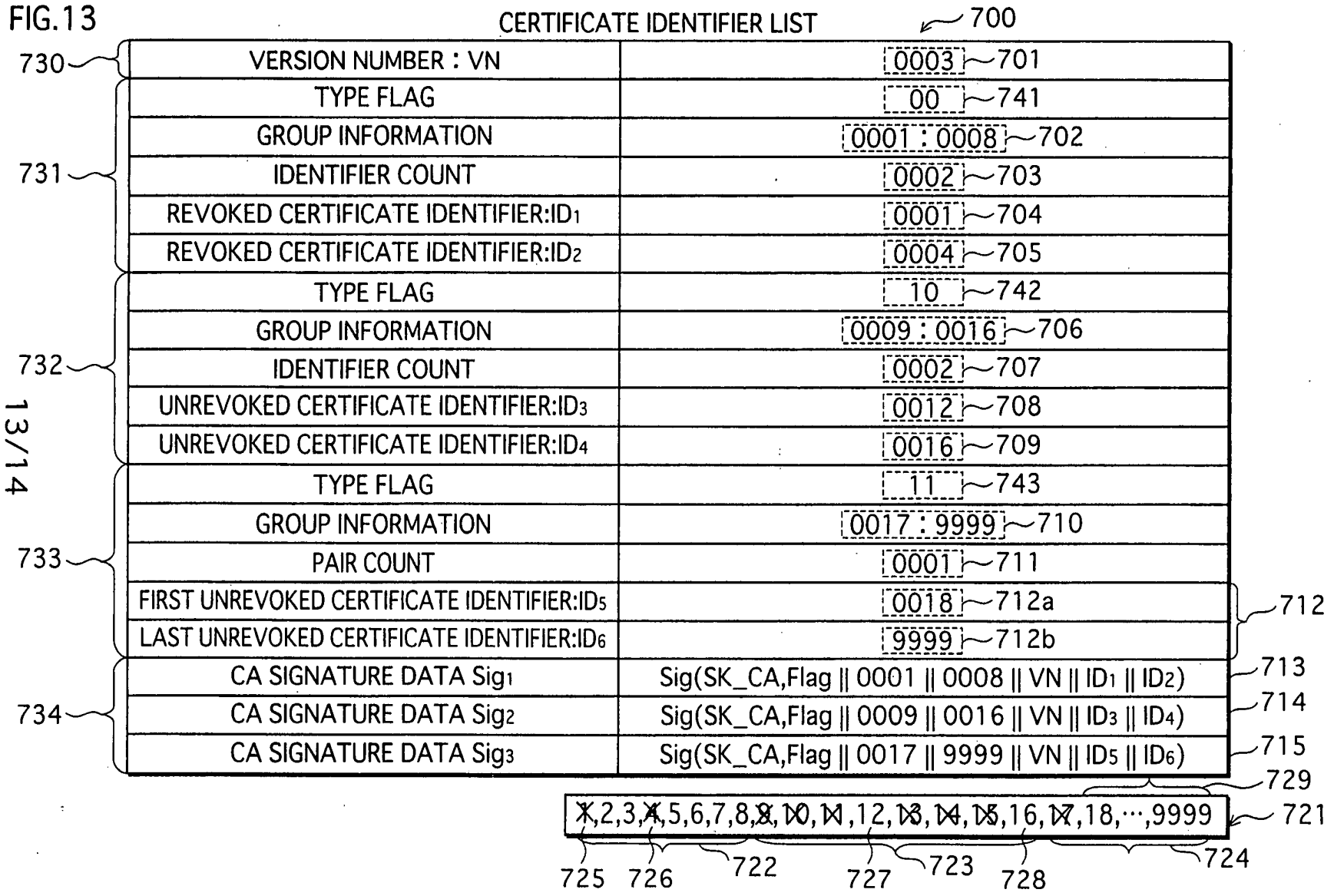
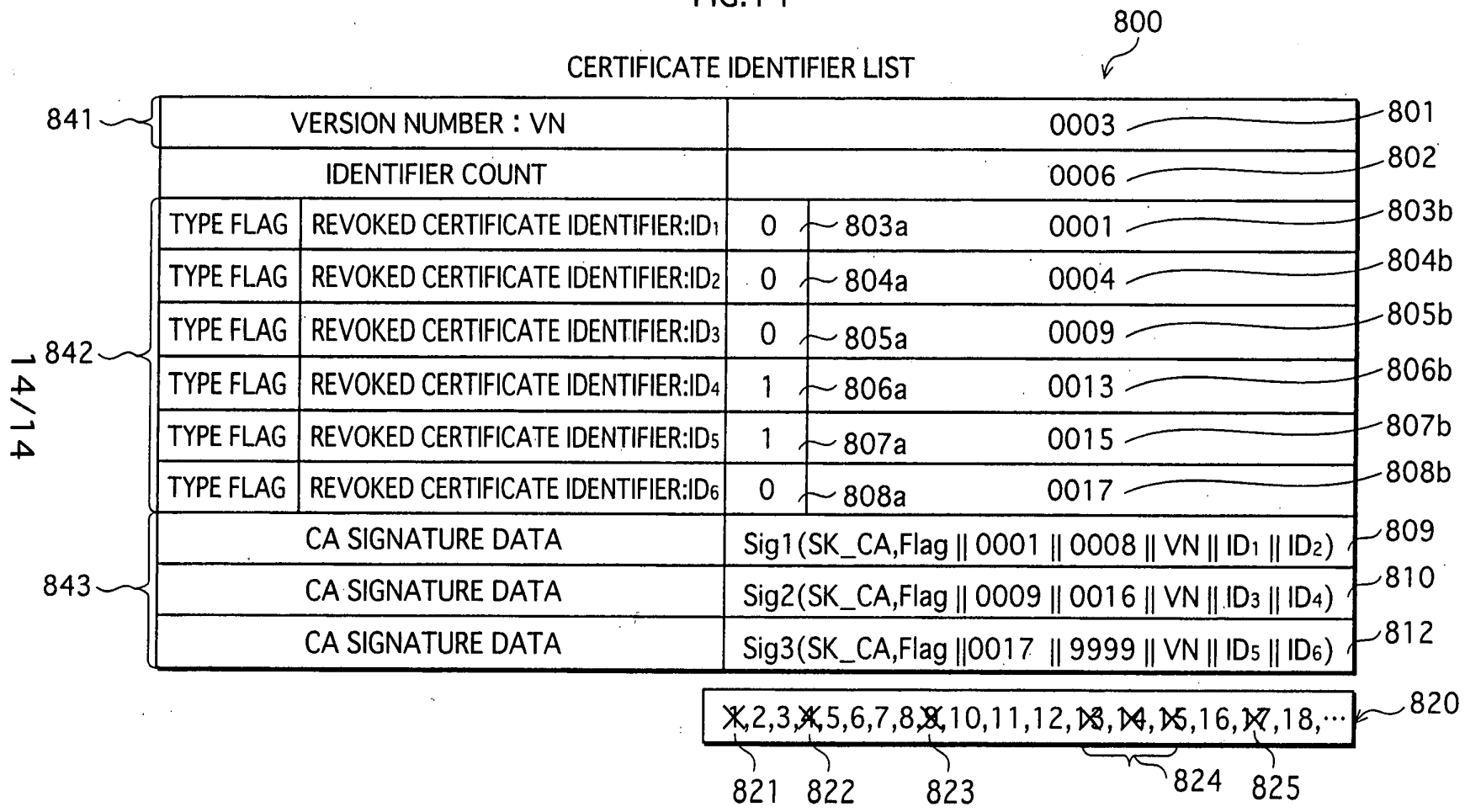

CERTIFICATE IDENTIFIER LIST
700
730
731
732
733
734
VERSION NUMBER : VN
0003
701
TYPE FLAG
00
741
GROUP INFORMATION
0001 : 0008
702
IDENTIFIER COUNT
0002
703
REVOKED CERTIFICATE IDENTIFIER:ID1
0001
704
REVOKED CERTIFICATE IDENTIFIER:ID2
0004
705
TYPE FLAG
10
742
GROUP INFORMATION
0009 : 0016
706
IDENTIFIER COUNT
0002
707
UNREVOKED CERTIFICATE IDENTIFIER:ID3
0012
708
UNREVOKED CERTIFICATE IDENTIFIER:ID4
0016
709
TYPE FLAG
11
743
GROUP INFORMATION
0017 : 9999
710
PAIR COUNT
0001
711
FIRST UNREVOKED CERTIFICATE IDENTIFIER:ID5
0018
712a
LAST UNREVOKED CERTIFICATE IDENTIFIER:ID6
9999
712b
712
CA SIGNATURE DATA Sig1
Sig(SK_CA,Flag || 0001 || 0008 || VN || ID1 || ID2)
713
CA SIGNATURE DATA Sig2
Sig(SK_CA,Flag || 0009 || 0016 || VN || ID3 || ID4)
714
CA SIGNATURE DATA Sig3
Sig(SK_CA,Flag || 0017 || 9999 || VN || ID5 || ID6)
715
729
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,…,9999
721
725
726
722
727
723
728
724

FIG.14


800
CERTIFICATE IDENTIFIER LIST
841
VERSION NUMBER : VN
0003
801
IDENTIFIER COUNT
0006
802
842
TYPE FLAG
REVOKED CERTIFICATE IDENTIFIER:ID1
0
803a
0001
803b
TYPE FLAG
REVOKED CERTIFICATE IDENTIFIER:ID2
0
804a
0004
804b
TYPE FLAG
REVOKED CERTIFICATE IDENTIFIER:ID3
0
805a
0009
805b
TYPE FLAG
REVOKED CERTIFICATE IDENTIFIER:ID4
1
806a
0013
806b
TYPE FLAG
REVOKED CERTIFICATE IDENTIFIER:ID5
1
807a
0015
807b
TYPE FLAG
REVOKED CERTIFICATE IDENTIFIER:ID6
0
808a
0017
808b
843
CA SIGNATURE DATA
Sig1(SK_CA,Flag || 0001 || 0008 || VN || ID1 || ID2)
809
CA SIGNATURE DATA
Sig2(SK_CA,Flag || 0009 || 0016 || VN || ID3 || ID4)
810
CA SIGNATURE DATA
Sig3(SK_CA,Flag ||0017 || 9999 || VN || ID5 || ID6)
812
1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,…
820
821
822
823
824
825